ABSTRACT

A method of detecting decryption of encrypted viral code is provided. Executable code in a subject file is emulated by a code emulator. A memory monitor monitors memory access information supplied by the emulator. A memory area that is read during emulation of an instruction in the code is flagged. Modification to the flagged memory area which was read is determined. The memory monitor determines whether a memory region that is contiguous with the modified memory area, and then updates the memory region to encompass the modified memory area. The memory monitor also determines whether the updated memory region is larger than a predetermined size to trigger viral detection. The detection method may be embodied in a computer system, in a computer program (or some unit of code) stored on a computer readable medium, such as a floppy disk, CD, DVD, etc., and/or transmitted via a network, such as the Internet, or another transmission medium.